

Intelligence Community Certification and Accreditation Transformation



Connect. Integrate. Collaborate.

Roger L. Caslow
IC CIO

Intelligence Community Information Assurance



The Bottom Line

- The Intelligence Community is working towards an *innovative* and *efficient* way to perform Security Authorization (also known as Certification and Accreditation (C&A)) across the *National Security Community*, establishing a single approach by:
 - Converging parallel efforts across the Federal Government
 - Leveraging partnerships
- We are working to ensure our approach is integrated with current activities and supported by:
 - Committee on National Security Systems (CNSS)
 - Department of Defense (DoD)
 - National Institute of Standards and Technology (NIST)
 - OMB Information Systems Security Line of Business (ISS LOB)
 - Program Manager-Information Sharing Environment (PM-ISE)
 - Unified Cross Domain Management Office (UCDMO)



Strategy

- **Incorporate security throughout the lifecycle**
- **Standardize the process and procedures**
- **Achieve reciprocity and reuse of documentation**



Transformation Goals



Establish a common set of trust levels



Achieve reciprocity



Define, document, and adopt common security controls



Develop a common language for efficient communication among security professionals, program managers, developers, and acquisition officials



Manage risk from an overall enterprise perspective addressing mission and budget as well as security



Incorporate Information Assurance (IA) into enterprise architecture and deliver IA services as enterprise services

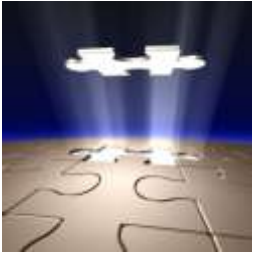


Build security into the “lifecycle” so that it becomes adaptable to different development environments.



Foundational Changes

S
T
R
A
T
E
G
Y



Risk Management

System

Enterprise

Governance

Passive/Intuitive

Active and repeatable

P
R
O
C
E
S
S



Standards and Guidelines

Inability to capture security-related costs

Integration and tracking of security costs

Budget

Multiple sets

Single set

Adaptability

Inflexible

Flexible

P
E
O
P
L
E



Roles and Responsibilities

Functional stovepipes

Integrated competencies

Leadership

Lack insight

Informed decisions

Knowledge

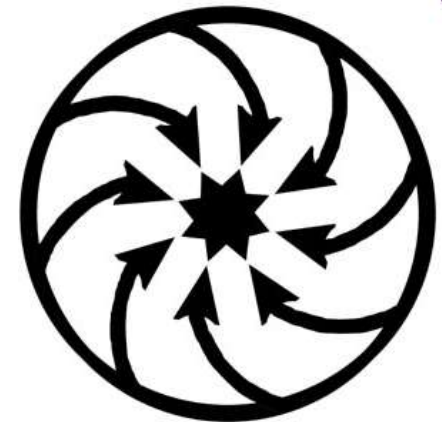
Functional expertise

Broad understanding



Unifying Federal Government Efforts

- **Certification and Accreditation is now a part of the Risk Management Framework**
 - Ensures security is built into the system lifecycle (SDLC)
 - Captured in both Civil and National Security-related documentation
- **Reciprocity and Reuse**
 - Intelligence Community - ICD 503
 - Between DoD and IC - Agreement signed between the DoD & IC CIOs
 - Among DoD Organizations – C&A Reciprocity Memorandum from DoD PAAs
- **NIST, IC, DoD and CNSS are working together**
 - Delivered NIST SP 800-53, CNSSI 1253, CNSSP 22, CNSSI, and a set of RMF related templates
 - Updating NIST SPs 800-39, 800-37, 800-30, 800-53A to formulate a single federal approach
- **Program Manager - Information Sharing Environment (PM-ISE)**
 - Partner with IC, DoD
 - Extending work to the state, local, tribal level



Risk Management Framework (RMF) Application

**NIST 800-53A /
NIST 800-37 / NIST800-30**
Continuously track changes to information system that may affect security controls and reassess control effectiveness

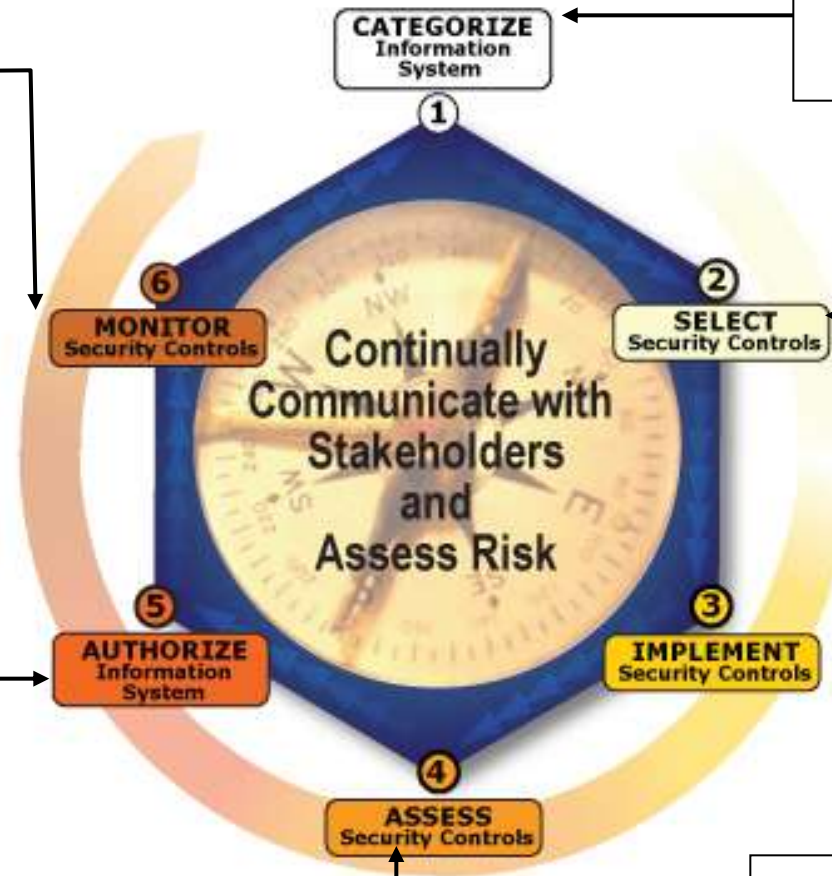
NIST 800-37/ CNSSI 1253
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

NIST SP 800-53 / CNSSI 1253
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk Assessment.

**NIST 800-39 / NIST 800-37
/ NIST 800-30**
Determine risk to organizational operations, assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

NIST 800-37
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

NIST SP 800-53A / NIST 800-37
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).



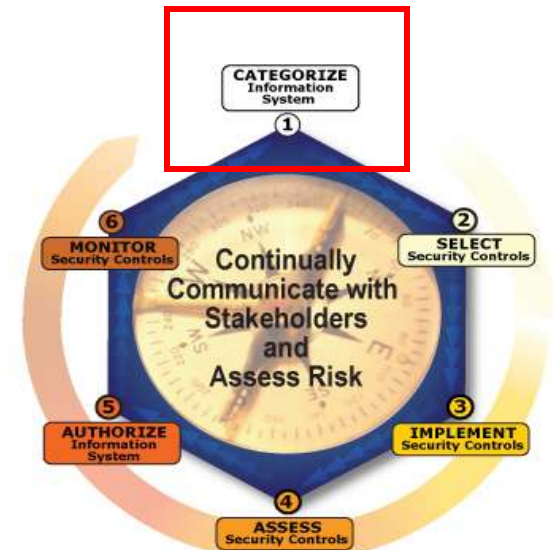
Need for New Policies and Guidance

- **Multiple policies for certification and accreditation of information systems among agencies, depending on information classification**
 - Director of Central Intelligence Directive (DCID) 6/3 for Sensitive Compartmented Information (SCI) systems
 - NISPOM, DICAP, or DIACAP for non-SCI classified systems
 - NIST for unclassified systems
- **Example: DCID 6/3**
 - Different interpretation and implementation by each agency
 - Fixed security requirements, without regard to business/mission
 - Documentation intensive
 - Documentation often redundant among different agencies
- **Interpreting the diversity of requirements and processes across organizations increases the time needed to develop and implement systems**



Categorize Overview

- Categorization is a risk-based characterization of information or information systems based on the potential impact of a loss of *confidentiality, integrity, or availability (C-I-A)*
- Three categories of potential impact
 - Low
 - Moderate
 - High
- CNSSI 1253 defines two categorization methodologies for NSS
 - Baseline-based (potential impact)
 - Control Profile-based



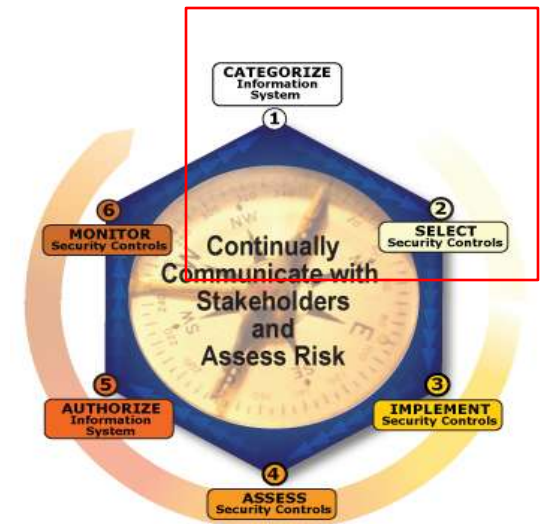
Select Overview

- Regardless of categorization method, controls are selected from the NIST SP 800-53 control catalog (Appendix F)
- The method for selecting controls for both NSS and non-NSS is described in detail in NIST SP 800-53, and is summarized for NSS in CNSSI 1253
- CNSSI 1253 provides unique selection guidance for NSS
 - Additional tailoring, supplementing guidance
 - NSS-unique controls baselines
 - NSS-unique variable instantiations



NIST SP 800-53 and CNSSI 1253

- **For National Security Systems**
 - Follow CNSSI 1253
 - To categorize the system
 - Baseline (Impact) Method
 - Control Profiles Method
 - To select the baseline set of security controls
 - To determine variable instantiations for Assignments
 - Follow NIST SP 800-53
 - For descriptions of all security controls (the controls catalog)
 - For initial guidance on the selection process (tailoring, supplementing)



Policy Doctrine

NIST

Brings the national security community closer to FISMA requirements

Assists with Inspector General (IG) audits, which are based on NIST standards

Aligns with rest of Federal Government to support reciprocity



Develop and use CNSS equivalents or supplements to NIST Publications

Unifies DoD and Intelligence Community (IC) with common standards and processes

Incorporates unique needs of national security community



Craft IC Implementations to address IC unique missions and requirements

Publication development time

Use of draft publications

Establish Intelligence Community Directives (ICD) and Standards (ICS)

Where necessary, draft Intelligence Community Standard supplements to Federal Information Processing Standards and NIST Special Publications



Intelligence Community Directive (ICD) 503

- ***ICD 503 “Information Technology Systems Security Risk Management, Certification and Accreditation”***
 - Signed by the DNI and effective on September 15, 2008
 - Rescinded DCID 6/3 Policy and Manual* and DCID 6/5 Manual
 - Addresses Policy for:
 - Risk Management
 - Accreditation
 - Certification
 - Reciprocity
 - Interconnections
 - Governance and Dispute Resolution

* Note: Appendix E remains in effect

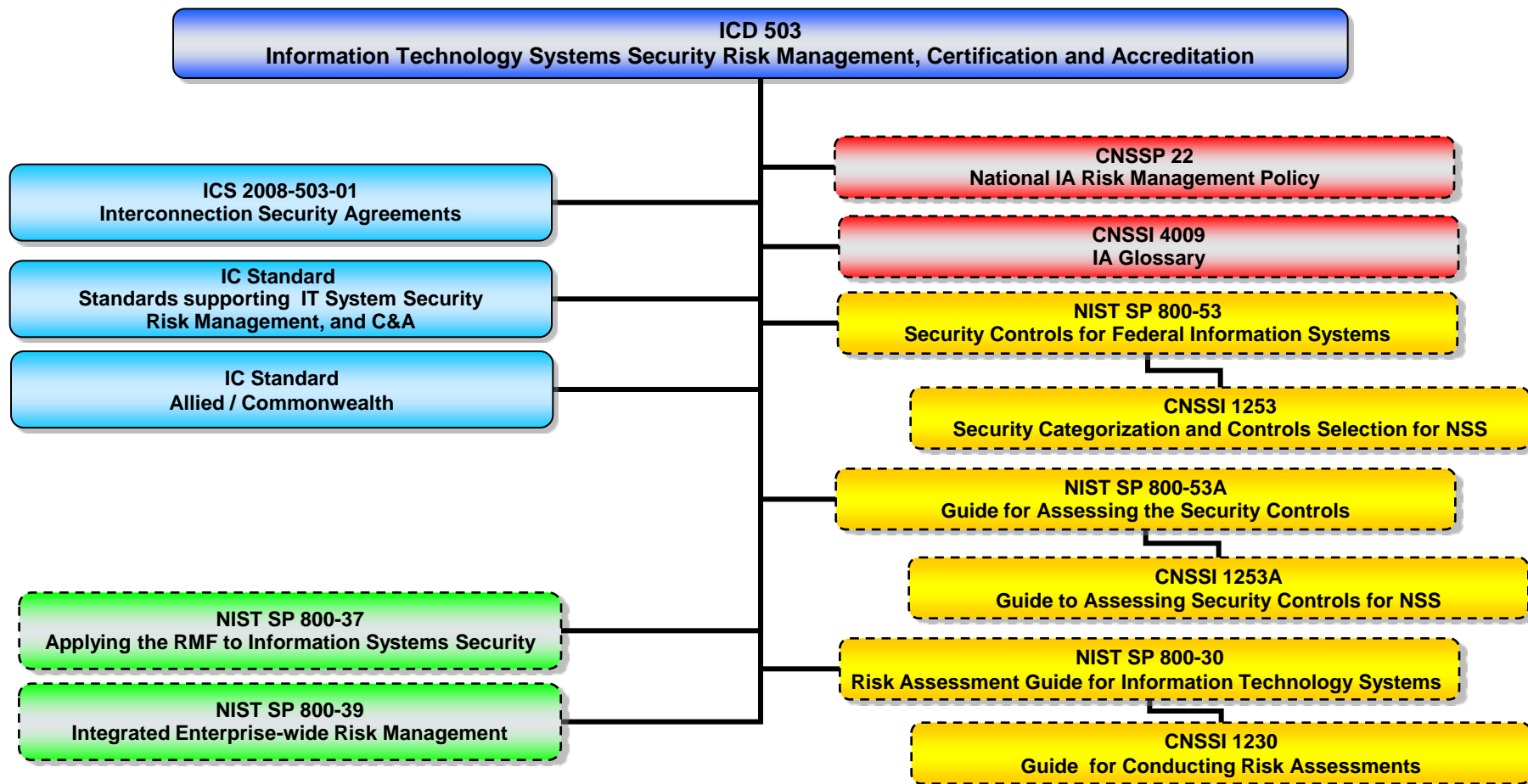


Key Elements of ICD 503

- Requires IC elements to determine level of acceptable risk based on a holistic perspective that considers Mission, Business and Security requirements
- Applies Consistent Standards for Risk Management
 - Promulgated by the IC CIO
 - Standards to include policies and guidelines approved by NIST and CNSS
- Calls for the application of a common security authorization process and standards for the IC Information Technology Enterprise
- Defines key roles in the C&A Process
 - Authorizing Official (AO)
 - Delegated Authorizing Official (DAO)
 - Certification Agent (CA)



IC Policy Structure



Policy architecture now leverages national-level documentation



Concerns on Transition

C&A Guidance

Policies/Standards

Technical Staffing

Resources

Transition implementation timelines

Performance Measures/Milestones

New Concepts



Transitioning...

Status (So What)

Now What

Then What

Valid accreditation (without liens) under DCID 6/3 that is less than three years old

Accreditation is “grandfathered”

Reaccreditation will be done under provisions of ICD 503

C&A review under DCID 6/3 provisions but not yet accredited

Complete C&A under provisions of DCID 6/3

Transition to ICD 503 and RMF where re-accreditation activities would normally begin

Accredited under DCID 6/3 with conditions (i.e., POA&M included)

Accreditation valid until approval expires or security relevant change triggers re-accreditation activities

Complete the POA&M actions as specified - Transition to ICD 503 for post-accreditation continuous monitoring








New system or scheduled for reaccreditation

Conduct certification under provisions of ICD 503

Conduct certification and accreditation activities in accordance with ICD 503 and RMF methodology



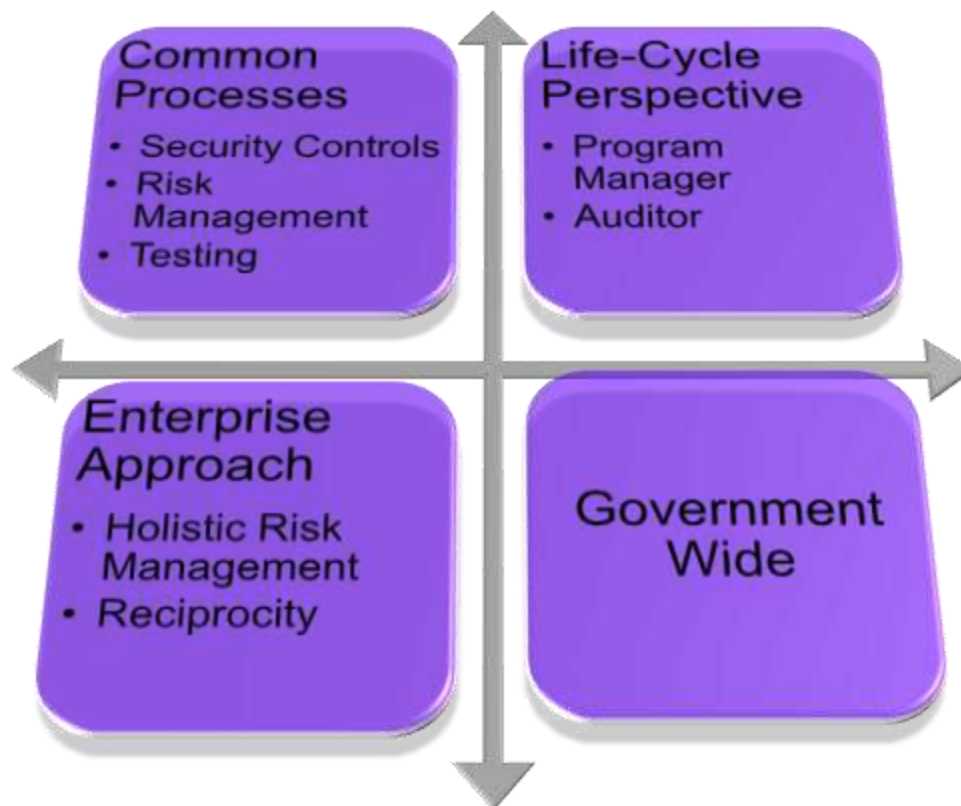
Timeline

	2010 Q2	2010 Q3	2010 Q4	2011	2012	2013	2014
Guidance Published							
Initiate / Continue Training							
Pilot new processes							
Acquire Tools							
Transition new systems							
Transition legacy systems							
Transition Complete							

- Timeline START begins with publication of the documents listed on slide 10 and assumes April 2010 start date
- Initiate Training: START + 2-6 months
- Pilot processes: START + 2-6 months (pilot should last approx 6 months)
- Transition of new systems (initiation phase of the lifecycle): Pilot + 6 months
- Acquire and apply automated tools (START + *availability*)
- Transition of legacy systems to ICD 503: Pilot + 3.5 years
- Transition complete: START + 4 years



IMPACT...



Questions



Contact Information

- **IC CIO Team:**
 - Roger Caslow, 703-983-3340
 - Jennifer Fabius Greene, 703-983-3449

- **Websites:**
 - Intelink-U website: <https://www.intelink.gov/ICTG/ca.intel>
 - Intelink-TS website: http://www.intelink.ic.gov/ICTG/ppd_ca.intel

